

Relational Database Service

Getting Started

Issue 01
Date 2022-09-30



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Getting Started with RDS for MySQL.....	1
1.1 Operation Guide.....	1
1.2 Step 1: Buy a DB Instance.....	2
1.3 Step 2: Connect to a DB Instance.....	7
1.3.1 Overview.....	7
1.3.2 Connecting to an RDS for MySQL DB Instance Through DAS (Recommended).....	10
1.3.3 Connecting to an RDS for MySQL DB Instance Through a Private Network.....	11
1.3.3.1 Overview.....	11
1.3.3.2 Connecting to a DB Instance from a Linux ECS.....	11
1.3.3.3 Connecting to a DB Instance from a Windows ECS.....	14
1.3.3.4 Configuring Security Group Rules.....	17
1.3.4 Connecting to an RDS for MySQL DB Instance Through a Public Network.....	19
1.3.4.1 Overview.....	19
1.3.4.2 Binding an EIP.....	20
1.3.4.3 Connecting to a DB Instance from a Linux ECS.....	21
1.3.4.4 Connecting to a DB Instance from a Windows Server.....	23
1.3.4.5 Configuring Security Group Rules.....	25
2 Getting Started with RDS for MariaDB.....	28
2.1 Operation Guide.....	28
2.2 Step 1: Buy a DB Instance.....	29
2.3 Step 2: Connect to a DB Instance.....	33
2.3.1 Overview.....	33
2.3.2 Connecting to a DB Instance Through a Private Network.....	35
2.3.2.1 Overview.....	35
2.3.2.2 Configuring Security Group Rules.....	36
2.3.2.3 Connecting to a DB Instance Using a MariaDB Client.....	39
2.3.3 Connecting to a DB Instance Through a Public Network.....	41
2.3.3.1 Overview.....	41
2.3.3.2 Binding an EIP.....	42
2.3.3.3 Configuring Security Group Rules.....	43
2.3.3.4 Connecting to a DB Instance Using a MariaDB Client.....	46
2.3.4 Connecting to a DB Instance Through DAS.....	48
3 Getting Started with RDS for PostgreSQL.....	49

3.1 Operation Guide.....	49
3.2 Step 1: Buy a DB Instance.....	50
3.3 Step 2: Connect to a DB Instance.....	55
3.3.1 Overview.....	55
3.3.2 Connecting to a DB Instance Through DAS (Recommended).....	58
3.3.3 Connecting to a DB Instance Through a Private Network.....	59
3.3.3.1 Overview.....	59
3.3.3.2 Connecting to a DB Instance from a Linux ECS.....	59
3.3.3.3 Configuring Security Group Rules.....	63
3.3.4 Connecting to a DB Instance Through a Public Network.....	64
3.3.4.1 Overview.....	64
3.3.4.2 Binding an EIP.....	65
3.3.4.3 Connecting to a DB Instance from a Linux ECS.....	66
3.3.4.4 Configuring Security Group Rules.....	69
A Change History	71

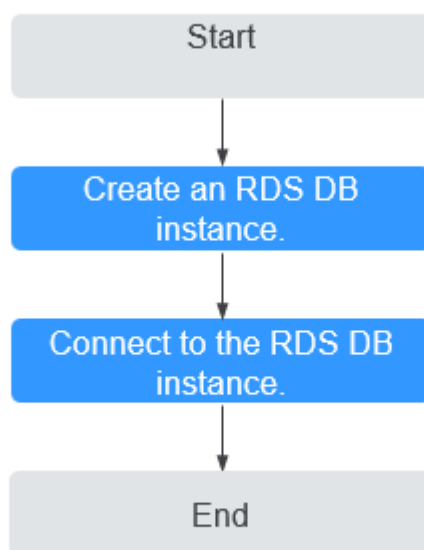
1 Getting Started with RDS for MySQL

1.1 Operation Guide

You can create and connect to DB instances on the RDS console.

Flowchart

Figure 1-1 Flowchart



Procedure

Table 1-1 Related operations and references

Operation	Reference
Creating an RDS DB instance	Step 1: Buy a DB Instance
Connecting to an RDS DB instance	Step 2: Connect to a DB Instance

1.2 Step 1: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the management console.

RDS allows you to tailor your compute resources and storage space to your business needs.

Procedure

- Step 1** Go to the [Buy DB Instance](#) page.
- Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.
- Billing mode
 - **Yearly/Monthly**: If you select this mode, skip [Step 3](#) and go to [Step 4](#).
 - **Pay-per-use**: If you select this mode, go to [Step 3](#).
 - Basic information

Table 1-2 Basic information

Parameter	Description
Region	Region where your resources are located. NOTE Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	Set to MySQL .

Parameter	Description
DB Engine Version	<p>Different DB engine versions are supported in different regions.</p> <p>When creating an RDS for MySQL instance, select a proper DB engine version tailored to your workloads. You are advised to select the latest available version because it is more stable, reliable, and secure.</p>
DB Instance Type and AZ	<ul style="list-style-type: none"> - Primary/Standby: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. - Single: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small and medium enterprises, or for learning about RDS.
Storage Type	<p>Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be.</p> <ul style="list-style-type: none"> - Cloud SSD: cloud drives used to decouple storage from compute. The maximum throughput is 350 MB/s. - Ultra-high I/O: uses the SSD disk type that supports a maximum throughput of 350 MB/s.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance.

- Specifications and storage

Table 1-3 Specifications and storage

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes support different numbers of database connections and maximum IOPS.

Parameter	Description
Storage Space (GB)	<p>Contains the file system overhead required for inode, reserved block, and database operation.</p> <p>NOTE</p> <ul style="list-style-type: none"> Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB.
Disk Encryption	<ul style="list-style-type: none"> Disable: Data stored in the disk is not encrypted. Enable: Enabling disk encryption improves data security, but slightly affects the read and write performance of the database. Key Name: indicates the tenant key. You can select an existing key or create a new one. <p>NOTE</p> <ul style="list-style-type: none"> After an instance is created, the disk encryption status and the key cannot be changed. For details about how to create a key, see the "Creating a CMK" section in the <i>Key Management Service User Guide</i>.

- Network and database configuration

Table 1-4 Network

Parameter	Description
VPC	<p>A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details on how to create a VPC, see "Creating a VPC" in <i>Virtual Private Cloud User Guide</i>.</p> <p>If no VPC is available, RDS allocates a VPC to you by default.</p> <p>NOTICE</p> <p>After a DB instance is created, the VPC cannot be changed.</p>
Subnet	<p>Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled.</p> <p>A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused IPv4 or IPv6 floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address.</p>

Parameter	Description
Security Group	<p>Enhances security by controlling access to RDS from other services. Ensure that the security group you select allows the client to access the DB instance.</p> <p>When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance.</p> <p>If no security group is available or has been created, RDS allocates a security group to you by default.</p>
Database Port	<p>The default database port is 3306. You can change it after a DB instance is created.</p> <p>RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017, 33071, and 33062, which are reserved for RDS system use.</p>

Table 1-5 Database configuration

Parameter	Description
Password	<ul style="list-style-type: none"> - Configure (default setting): Configure a password for your DB instance during the creation process. - Skip: Configure a password later after the DB instance is created. <p>NOTICE If you select Skip for Password, you need to reset the password before you can log in to the instance.</p>
Administrator	The default login name for the database is root .
Administrator Password	<p>Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#\$\$%^*_-=+?,()&).</p> <p>Enter a strong password and periodically change it for security reasons.</p> <p>If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password.</p> <p>Keep this password secure. The system cannot retrieve it.</p>
Confirm Password	Must be the same as Administrator Password .

Parameter	Description
Parameter Template	<p>Contains engine configuration values that can be applied to one or more DB instances. If you intend to create a primary/standby DB pair, they use the same parameter template.</p> <p>NOTICE If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used.</p> <ul style="list-style-type: none"> - back_log - innodb_io_capacity_max - max_connections - innodb_io_capacity - innodb_buffer_pool_size - innodb_buffer_pool_instances
Table Name	<p>Specifies whether table names are case sensitive. This parameter is supported for RDS for MySQL 8.0 only.</p> <p>The case sensitivity of table names for created RDS for MySQL 8.0 instances cannot be changed.</p>
Enterprise Project	<p>If your account has been associated with an enterprise project, select the target project from the Enterprise Project drop-down list.</p>

- Tags

Table 1-6 Tags

Parameter	Description
Tag	<p>Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance.</p>

- Purchase period

Table 1-7 Purchase period

Parameter	Description
Required Duration	<p>This option is available only for yearly/monthly DB instances. The system will automatically calculate the configuration fee based on the selected required duration. The longer the required duration is, the larger discount you will enjoy.</p>

Parameter	Description
Auto-renew	<ul style="list-style-type: none"> - This option is available only for yearly/monthly DB instances and is not selected by default. - If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	RDS supports batch creation of DB instances. If you intend to create primary/standby DB instances and set Quantity to 1 , a primary DB instance and a synchronous standby DB instance will be created.

 **NOTE**

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications for pay-per-use DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

Skip [Step 4](#) and [Step 5](#) and go to [Step 6](#).

Step 4 Confirm the order for yearly/monthly DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Pay Now**.

Step 5 Select a payment method and complete the payment.

 **NOTE**

This operation applies only to the yearly/monthly billing mode.

Step 6 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created. To view the detailed progress and result of the creation, go to the **Task Center** page.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- The default database port is **3306**. You can change it after a DB instance is created.

----End

1.3 Step 2: Connect to a DB Instance

1.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 1-8 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address is required. You can connect to your DB instance through DAS on the management console.	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	<ul style="list-style-type: none"> • Easy to use, secure, advanced, and intelligent • Recommended
Private network	Floating IP	<p>RDS provides a floating IP address by default.</p> <p>When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.</p>	<ul style="list-style-type: none"> • Secure and excellent performance • Recommended

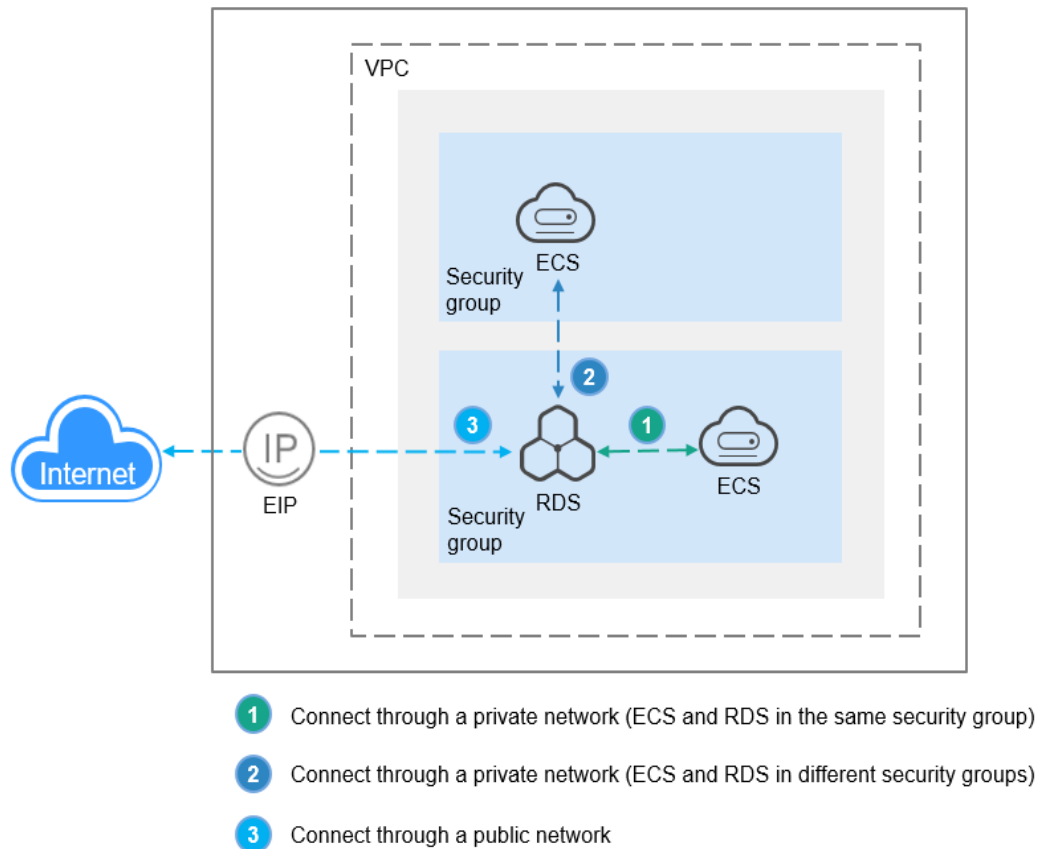
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	<ul style="list-style-type: none"> • A relatively lower level of security compared to other connection methods • To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance.

 **NOTE**

- VPC: Virtual Private Cloud
- ECS: Elastic Cloud Server
- EIP: Elastic IP
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 1-2 illustrates the connection over a private network or a public network.

Figure 1-2 DB instance connection




1.3.2 Connecting to an RDS for MySQL DB Instance Through DAS (Recommended)

Scenarios

Data Admin Service (DAS) enables you to connect to and manage DB instances with ease on a web-based console. The permission required for connecting to DB instances through DAS has been enabled for you by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.

Alternatively, click the DB instance name on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Step 4 On the displayed login page, enter the username and password and click **Log In**.
----End

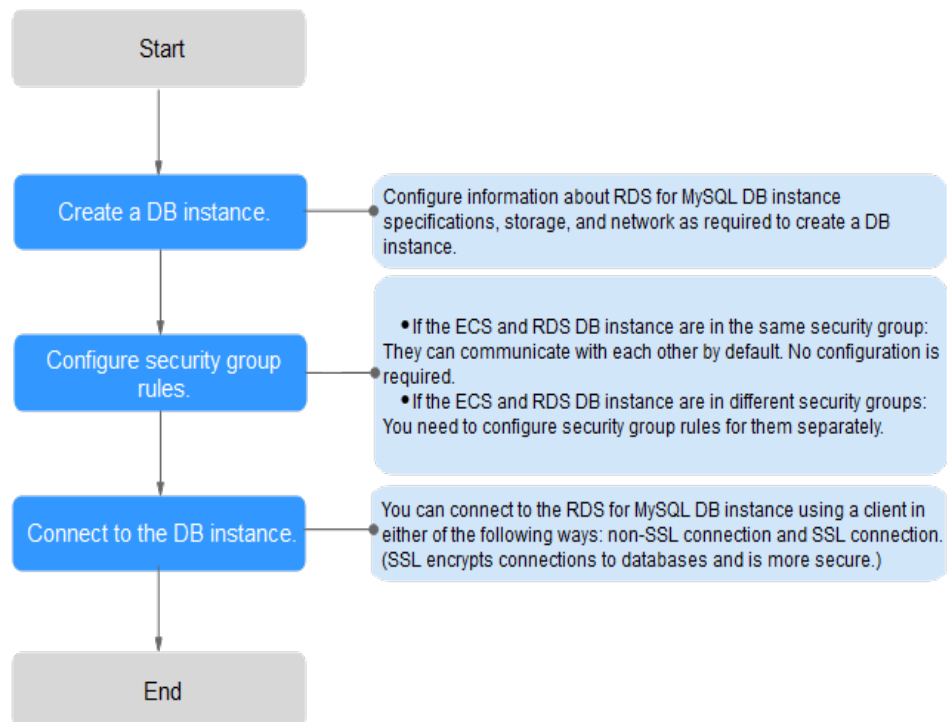
1.3.3 Connecting to an RDS for MySQL DB Instance Through a Private Network

1.3.3.1 Overview

Process

Figure 1-3 illustrates the process of connecting to an RDS for MySQL DB instance through a private network.

Figure 1-3 Connecting to a DB instance through a private network



1.3.3.2 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a MySQL client over a private network.

- **Step 1: Buy an ECS**
- **Step 2: Test Connectivity and Install a MySQL Client**
- **Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)**

Step 1: Buy an ECS

1. Log in to the management console and check whether there is an ECS available.

- If there is a Linux ECS, go to [3](#).
 - If there is a Windows ECS, see [Connecting to a DB Instance from a Windows ECS](#).
 - If no ECS is available, go to [2](#).
2. Buy an ECS and select Linux (for example, CentOS) as its OS.
To download a MySQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for MySQL DB instance for mutual communications.
For details about how to purchase a Linux ECS, see "Purchasing an ECS" in *Elastic Cloud Server User Guide*.
 3. On the **ECS Information** page, view the region and VPC of the ECS.
 4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.
 5. Check whether the ECS and RDS for MySQL instance are in the same region and VPC.
 - If yes, go to [Step 2: Test Connectivity and Install a MySQL Client](#).
 - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
 - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see "Changing a VPC" in the *Elastic Cloud Server User Guide*.

Step 2: Test Connectivity and Install a MySQL Client

1. Log in to the ECS. For details, see "Login Using VNC" in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.
4. On the ECS, check whether the floating IP address and database port of the DB instance can be connected.
telnet 192.168.6.144 3306
 - If yes, network connectivity is available.
 - If no, check the security group rules.
 - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.
 - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see [Configuring Security Group Rules](#).

- Download the MySQL client installation package for Linux to the ECS. The package `mysql-community-client-5.7.38-1.el6.x86_64.rpm` is used as an example.

A MySQL client running a version later than that of the DB instance is recommended.

```
wget https://dev.mysql.com/get/mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

- Install the MySQL client.

```
rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

 NOTE

- If any conflicts occur during the installation, add the `replacefiles` parameter to the command and install the client again.

```
rpm -ivh --replacefiles mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

- If a message is displayed prompting you to install a dependency package during the installation, add the `nodeps` parameter to the command and install the client again.

```
rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)

- Run the following command on the ECS to connect to the DB instance:

```
mysql -h <host> -P <port> -u <userName> -p
```

Example:

```
mysql -h 192.168.6.144 -P 3306 -u root -p
```

Table 1-9 Parameter description

Parameter	Description
<code><host></code>	Floating IP address obtained in 3 .
<code><port></code>	Database port obtained in 3 . The default value is 3306.
<code><userName></code>	Administrator account <code>root</code> .

- Enter the password of the database account if the following information is displayed:

Enter password:

Figure 1-4 Connection successful

```
[root@ecs-e5d6-test ~]# mysql -h 192.168.6.144 -P 3306 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108609
Server version: 5.7.38 MySQL Community Server - (GPL)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

1.3.3.3 Connecting to a DB Instance from a Windows ECS

You can connect to your DB instance using a Windows ECS installed with a database client (for example, MySQL-Front) over a private network.

- [Step 1: Buy an ECS](#)
- [Step 2: Test Connectivity and Install MySQL-Front](#)
- [Step 3: Connect to the DB Instance Using MySQL-Front](#)

Step 1: Buy an ECS

1. Log in to the management console and check whether there is an ECS available.
 - If there is a Linux ECS, see [Connecting to a DB Instance from a Linux ECS](#).
 - If there is a Windows ECS, go to [3](#).
 - If no ECS is available, go to [2](#).
2. Buy an ECS and select Windows as its OS.

To download a MySQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for MySQL DB instance for mutual communications.

For details about how to purchase a Windows ECS, see "Purchasing an ECS" in *Elastic Cloud Server User Guide*.
3. On the **ECS Information** page, view the region and VPC of the ECS.
4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.
5. Check whether the ECS and RDS for MySQL instance are in the same region and VPC.
 - If yes, go to [Step 2: Test Connectivity and Install MySQL-Front](#).
 - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
 - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see "Changing a VPC" in the *Elastic Cloud Server User Guide*.

Step 2: Test Connectivity and Install MySQL-Front

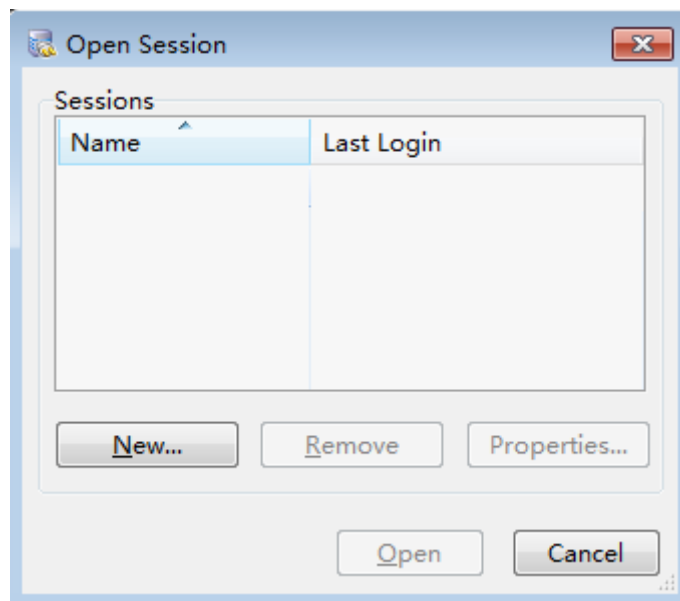
1. Log in to the ECS. For details, see "Login Using VNC" in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.
4. Open the cmd window on the ECS and check whether the floating IP address and database port of the DB instance can be connected.
telnet 192.168.6.144 3306

- If yes, network connectivity is available.
 - If no, check the security group rules.
 - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.
 - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see [Configuring Security Group Rules](#).
5. Open a browser, and download and install the MySQL-Front tool on the ECS (version 5.4 is used as an example).

Step 3: Connect to the DB Instance Using MySQL-Front

1. Start MySQL-Front.
2. In the displayed dialog box, click **New**.

Figure 1-5 Connection management



3. Enter the information of the DB instance to be connected and click **Ok**.

Figure 1-6 Adding an account

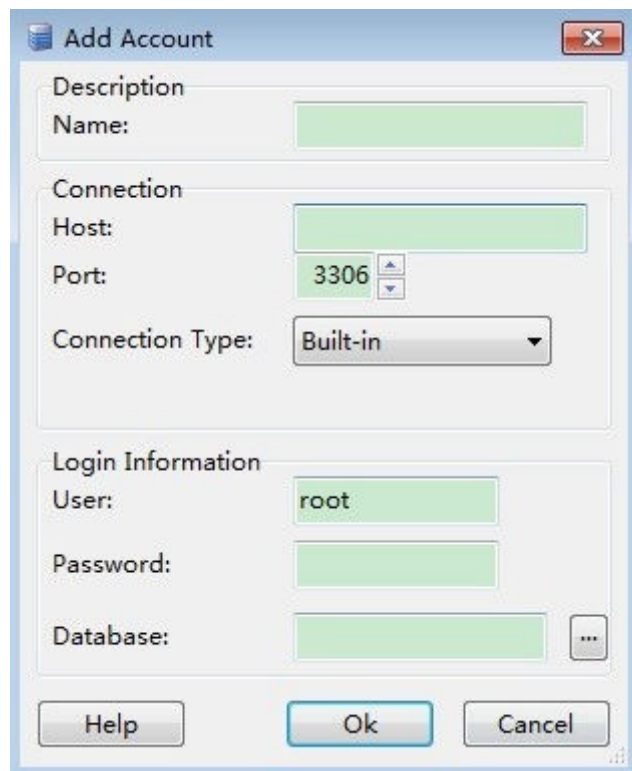
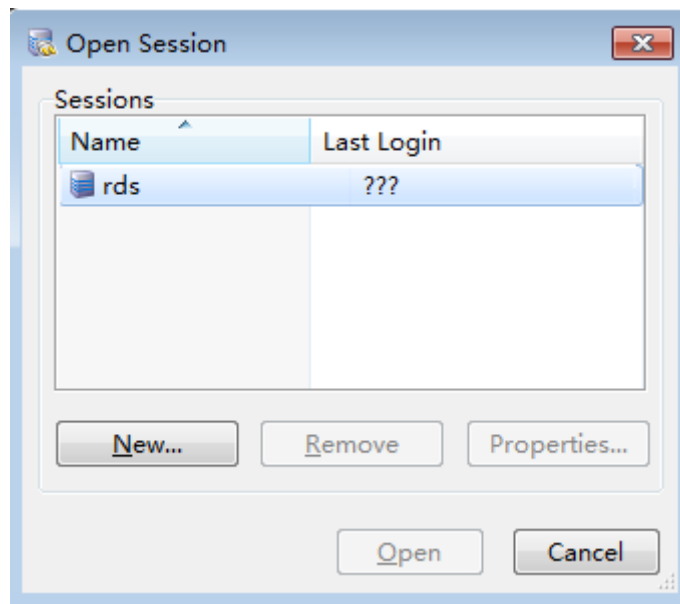


Table 1-10 Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not specify this parameter, it will be the same as that configured for Host by default.
Host	Floating IP address obtained in 3 .
Port	Database port obtained in 3 . The default value is 3306.
User	Name of the user who will access the DB instance. The default user is root .
Password	Password of the account for accessing the DB instance.

- In the displayed window, select the connection that you have created in [3](#) and click **Open**. If the connection information is correct, the DB instance will be connected.

Figure 1-7 Opening a session



1.3.3.4 Configuring Security Group Rules

Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted within a VPC.

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance from a Linux ECS](#).
- If they are in different security groups, configure security group rules for them, separately.
 - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
 - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.


- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated with multiple security groups, and one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

 **NOTE**

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the DB instance name.

Step 4 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name to view the security group rules.

Step 5 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click .

 **NOTE**

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Table 1-11 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	Protocol: network protocol. Available options: All, TCP, UDP, ICMP, or GRE.	Custom TCP
	Port: the port over which the traffic can reach your DB instance. RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306

Parameter	Description	Example Value
Type	IP address type. <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: <ul style="list-style-type: none"> • Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) • All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) • IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) • Security group: default_securitygroup 	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	N/A

----End

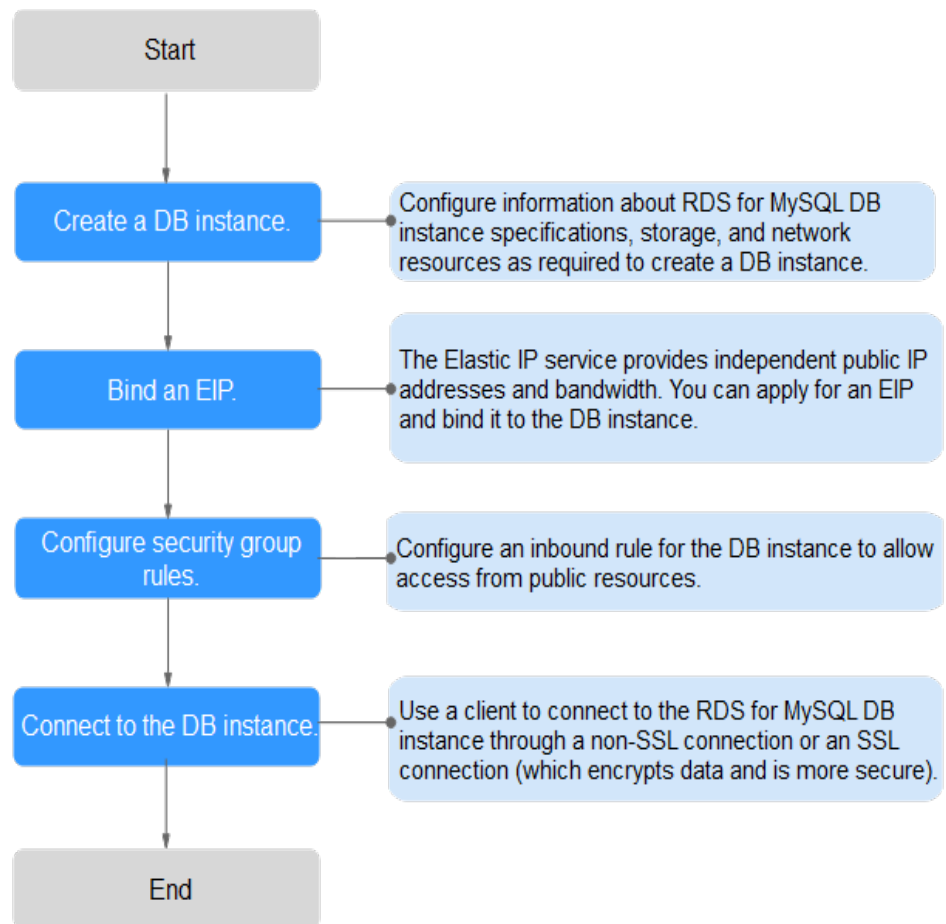
1.3.4 Connecting to an RDS for MySQL DB Instance Through a Public Network

1.3.4.1 Overview

Process

Figure 1-8 illustrates the process of connecting to an RDS for MySQL DB instance through a public network.

Figure 1-8 Connecting to a DB instance through a public network



1.3.4.2 Binding an EIP


Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see [Configuring Security Group Rules](#).
- Public accessibility reduces the security of DB instances. Therefore, exercise caution when enabling this function. To achieve a higher transmission rate and security level, you are advised to migrate your applications to the ECS that is in the same region as RDS.

Binding an EIP

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.
- Step 3** On the **Instances** page, click the target DB instance.
- Step 4** In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.
- Step 5** In the displayed dialog box, select an EIP and click **Yes**.
- Step 6** On the **Connectivity & Security** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

1.3.4.3 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a MySQL client over a public network.

- [Step 1: Buy an ECS](#)
- [Step 2: Test Connectivity and Install a MySQL Client](#)
- [Step 3: Connect to the DB Instance Using Commands \(Non-SSL Connection\)](#)

Step 1: Buy an ECS

1. Log in to the management console and check whether there is an ECS available.
 - If there is a Linux ECS, go to [3](#).
 - If there is a Windows ECS, see [Connecting to a DB Instance from a Windows Server](#).
 - If no ECS is available, go to [2](#).
2. Buy an ECS and select Linux (for example, CentOS) as its OS.
To download a MySQL client to the ECS, bind an EIP to the ECS.
For details about how to purchase a Linux ECS, see "Purchasing an ECS" in *Elastic Cloud Server User Guide*.
3. On the **ECS Information** page, view the region and VPC of the ECS.
4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.

Step 2: Test Connectivity and Install a MySQL Client

1. Log in to the ECS. For details, see "Login Using VNC" in the *Elastic Cloud Server User Guide*.

2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.
If no EIP has been bound to the DB instance, see [Binding an EIP](#).
4. On the ECS, check whether the EIP and database port of the DB instance can be connected.

telnet *EIP 3306*

- If yes, network connectivity is available.
- If no, check the security group rules.
 - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the EIP and port of the DB instance.
 - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS.
For details, see [Configuring Security Group Rules](#).

5. Download the MySQL client installation package for Linux on the ECS. The `mysql-community-client-5.7.38-1.el6.x86_64.rpm` package is used as an example.

A MySQL client running a version later than that of the DB instance is recommended.

wget https://dev.mysql.com/get/mysql-community-client-5.7.38-1.el6.x86_64.rpm

6. Install the MySQL client.

rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

 **NOTE**

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and install the client again.

rpm -ivh --replacefiles mysql-community-client-5.7.38-1.el6.x86_64.rpm

- If a message is displayed prompting you to install a dependency package during the installation, add the **nodeps** parameter to the command and install the client again.

rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)

1. Run the following command on the ECS to connect to the DB instance:

mysql -h <host> -P <port> -u <userName> -p

Example:

mysql -h 192.168.0.1 -P 3306 -u root -p

Table 1-12 Parameter description

Parameter	Description
<code><host></code>	EIP obtained in 3 .

Parameter	Description
<port>	Database port obtained in 3. The default value is 3306.
<userName>	Administrator account root .

2. Enter the password of the database account if the following information is displayed:
Enter password:

Figure 1-9 Connection successful

```
[root@ecs-e5d6-test ~]# mysql -h  -P 3306 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108609
Server version:  MySQL Community Server - (GPL)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

1.3.4.4 Connecting to a DB Instance from a Windows Server

You can connect to your DB instance from a local Windows server installed with a database client (for example, MySQL-Front) over a public network.

- [Step 1: Test Connectivity and Install MySQL-Front](#)
- [Step 2: Connect to the DB Instance Using MySQL-Front](#)

Step 1: Test Connectivity and Install MySQL-Front

1. On the **Instances** page, click the DB instance name.
2. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.

If no EIP has been bound to the DB instance, see [Binding an EIP](#).

3. Open the cmd window on your local server and check whether the EIP and database port of the DB instance can be connected.

telnet *EIP 3306*

- If yes, network connectivity is available.
- If no, check the security group rules.

Check inbound rules in the security group of the DB instance. Add an inbound rule for the EIP and port of the DB instance. For details, see [Configuring Security Group Rules](#).

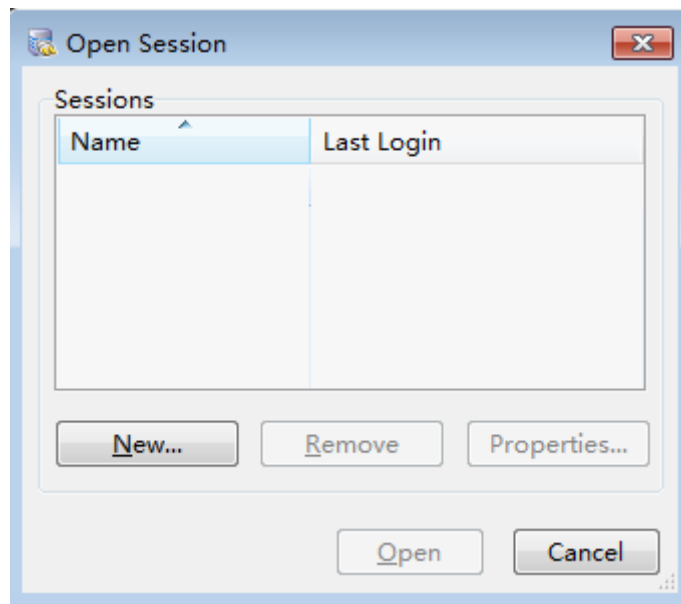
4. Open a browser, and download and install the MySQL-Front tool locally (version 5.4 is used as an example).

Step 2: Connect to the DB Instance Using MySQL-Front

1. Start MySQL-Front.

2. In the displayed dialog box, click **New**.

Figure 1-10 Connection management



3. Enter the information of the DB instance to be connected and click **Ok**.

Figure 1-11 Adding an account

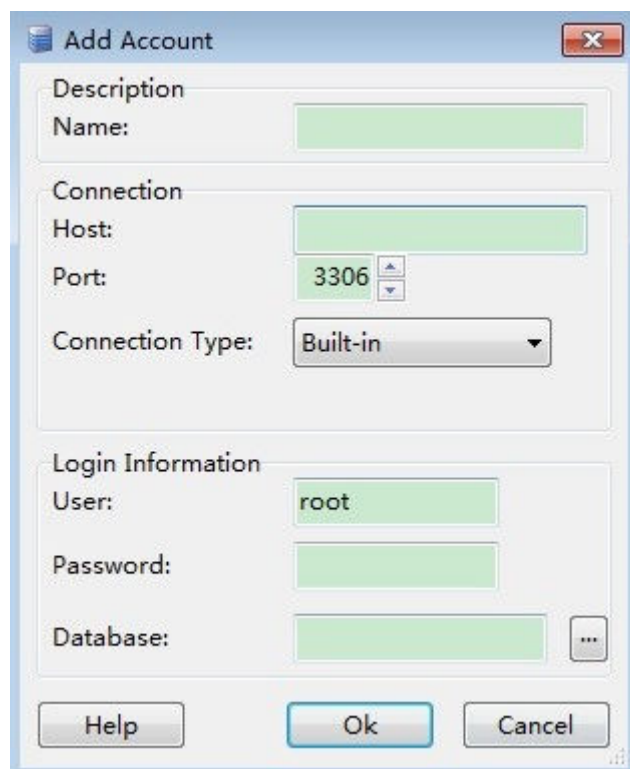
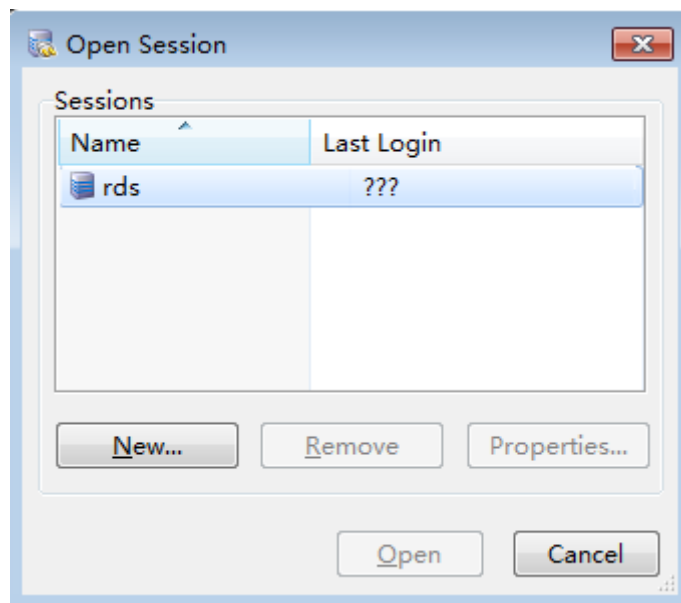


Table 1-13 Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not specify this parameter, it will be the same as that configured for Host by default.
Host	EIP obtained in 2.
Port	Database port obtained in 2. The default value is 3306.
User	Name of the user who will access the DB instance. The default user is root .
Password	Password of the account for accessing the DB instance.

- In the displayed window, select the connection that you have created in 3 and click **Open**. If the connection information is correct, the DB instance will be connected.

Figure 1-12 Opening a session



1.3.4.5 Configuring Security Group Rules

Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted within a VPC.

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

When you attempt to connect to an RDS DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.


- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated with multiple security groups, and one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the DB instance name.

Step 4 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name to view the security group rules.

Step 5 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click .

NOTE

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Table 1-14 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	Protocol: network protocol. Available options: All, TCP, UDP, ICMP, or GRE.	Custom TCP

Parameter	Description	Example Value
	<p>Port: the port over which the traffic can reach your DB instance.</p> <p>RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.</p>	3306
Type	<p>IP address type.</p> <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Source	<p>Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples:</p> <ul style="list-style-type: none"> • Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) • All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) • IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) • Security group: default_securitygroup 	0.0.0.0/0
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).</p>	N/A

----End

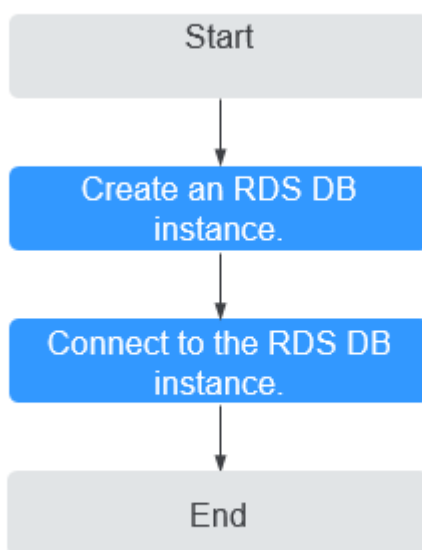
2 Getting Started with RDS for MariaDB

2.1 Operation Guide

You can create and connect to DB instances on the RDS console.

Flowchart

Figure 2-1 Flowchart



Procedure

Table 2-1 Related operations and references

Operation	Reference
Creating an RDS DB instance	Step 1: Buy a DB Instance
Connecting to an RDS DB instance	Step 2: Connect to a DB Instance

2.2 Step 1: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the RDS console.

RDS for MariaDB only supports the pay-per-use billing mode. RDS allows you to tailor your compute resources and storage space to your business needs.

Procedure

Step 1 Go to the [Buy DB Instance](#) page.

Step 2 On the displayed page, select a billing mode, configure information about your DB instance, and click **Next**.

- Billing mode: pay-per-use
- Basic information

Figure 2-2 Basic information

The screenshot displays the 'Basic information' configuration page for a new RDS instance. The settings are as follows:

- Billing Mode:** Yearly/Monthly/Pay-per-use (selected)
- Region:** AP-Bangkok
- DB Instance Name:** rds-abc
- DB Engine:** MySQL/PostgreSQL/Microsoft SQL Server/MariaDB (selected)
- DB Engine Version:** 10.5
- DB Instance Type:** Primary/Standby/Single (selected)
- Storage Type:** Cloud SSD
- Primary AZ:** az2
- Standby AZ:** az2
- Time Zone:** (UTC+08:00) Beijing, Chongqing, Hong...

Table 2-2 Basic information

Parameter	Description
Region	Region where your resources are located. NOTE Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	MariaDB
DB Engine Version	The DB engine version differs in different regions.
DB Instance Type	<ul style="list-style-type: none"> - Primary/Standby: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. - Single: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is only recommended for development and testing of microsites, and small and medium enterprises, or for learning about RDS.
AZ	An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. You can deploy primary and standby instances in a single AZ or across AZs to achieve failover and high availability.
Storage Type	Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be. Cloud SSD: cloud drives used to decouple storage from compute. The maximum throughput is 350 MB/s.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it later as needed.

- Specifications and storage

Figure 2-3 Specifications and storage

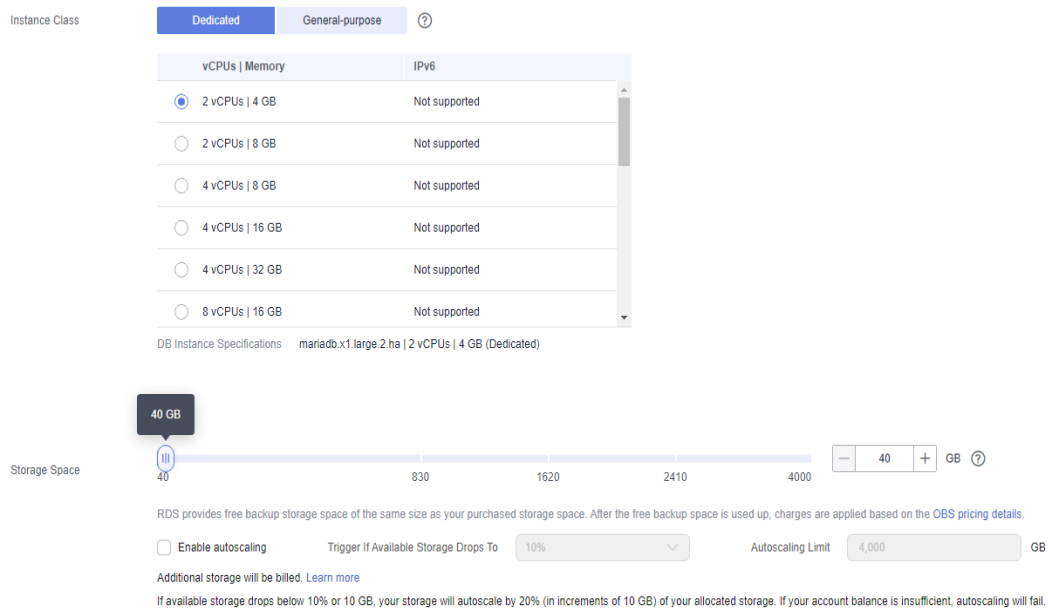


Table 2-3 Specifications and storage

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes have different numbers of database connections and different maximum IOPS.
Storage Space (GB)	Contains the system overhead required for inodes, reserved blocks, and database operation.

- Network and database configuration

Table 2-4 Network

Parameter	Description
VPC	<p>A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details about how to create a VPC, see "Creating a VPC" in <i>Virtual Private Cloud User Guide</i>.</p> <p>If no VPC is available, RDS allocates a VPC to you by default.</p> <p>NOTICE After a DB instance is created, the VPC cannot be changed.</p>

Parameter	Description
Subnet	<p>Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled.</p> <p>A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused IPv4 floating IP address in the subnet CIDR block.</p>
Security Group	<p>Enhances security by controlling access to RDS from other services. Ensure that the security group you select allows the client to access the DB instance.</p> <p>If no security group is available or has been created, RDS allocates a security group to you by default.</p>

Table 2-5 Database configuration

Parameter	Description
Administrator	The default login name for the database is root .
Administrator Password	<p>Must consist of 8 to 32 characters and contain the following character types: uppercase letters, lowercase letters, digits, and special characters (~!@#\$%^*_-=+?,()&). Enter a strong password and periodically change it for security reasons.</p> <p>If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password.</p> <p>Keep this password secure. The system cannot retrieve it.</p>
Confirm Password	Must be the same as Administrator Password .
Parameter Template	Contains engine configuration values that can be applied to one or more DB instances. If you intend to create a primary/standby DB pair, they use the same parameter template.
Table Name	<p>Specifies whether table names are case sensitive.</p> <p>NOTE The case sensitivity of table names for created instances cannot be changed.</p>
Enterprise Project	If your account has been associated with an enterprise project, select the target project from the Enterprise Project drop-down list.

- Tags

Table 2-6 Tags

Parameter	Description
Tag	Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance.

- Purchase period

Table 2-7 Purchase period

Parameter	Description
Quantity	RDS supports DB instance creation in batches. If you choose to create primary/standby DB instances and set Quantity to 1 , a primary DB instance and a standby DB instance will be created synchronously.

 **NOTE**

- The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications.

- If you need to modify your settings, click **Previous**.

Step 4 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created. To view the detailed progress and result of the creation, go to the **Task Center** page.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- After a DB instance is created, you can enter a description for it.
- The default database port is **3306**. You can change it after a DB instance is created.

----End

2.3 Step 2: Connect to a DB Instance

2.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 2-8 RDS connection methods

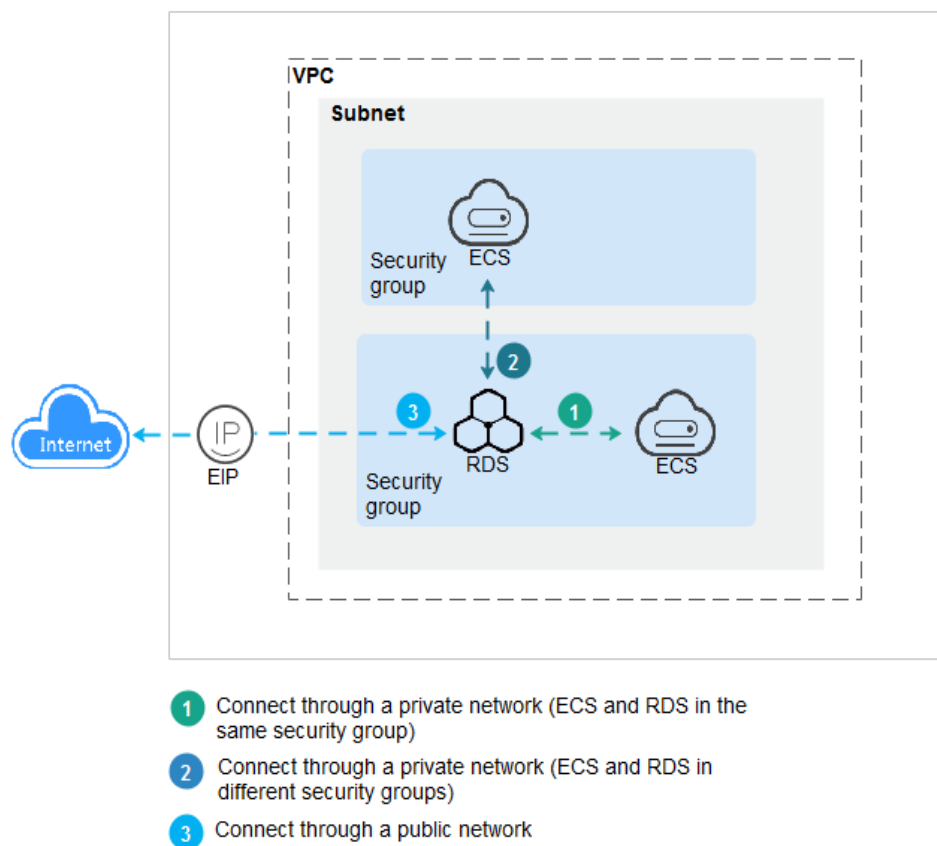
Connect Through	IP Address	Scenarios	Description
DAS	No IP address required	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	<ul style="list-style-type: none"> • Easy to use, secure, advanced, and intelligent • Recommended
Private network	Floating IP	<p>RDS provides a floating IP address by default.</p> <p>If your applications are deployed on an ECS that is in the same region and VPC as your DB instance, you are advised to use a floating IP address to connect to the DB instance through the ECS.</p>	<ul style="list-style-type: none"> • Secure and excellent performance • Recommended
Public network	EIP	If you cannot access a DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	<ul style="list-style-type: none"> • A relatively lower level of security compared to other connection methods • To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance.

NOTE

- VPC: Virtual Private Cloud
- ECS: Elastic Cloud Server
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 2-4 illustrates the connection over a private network or a public network.

Figure 2-4 DB instance connection



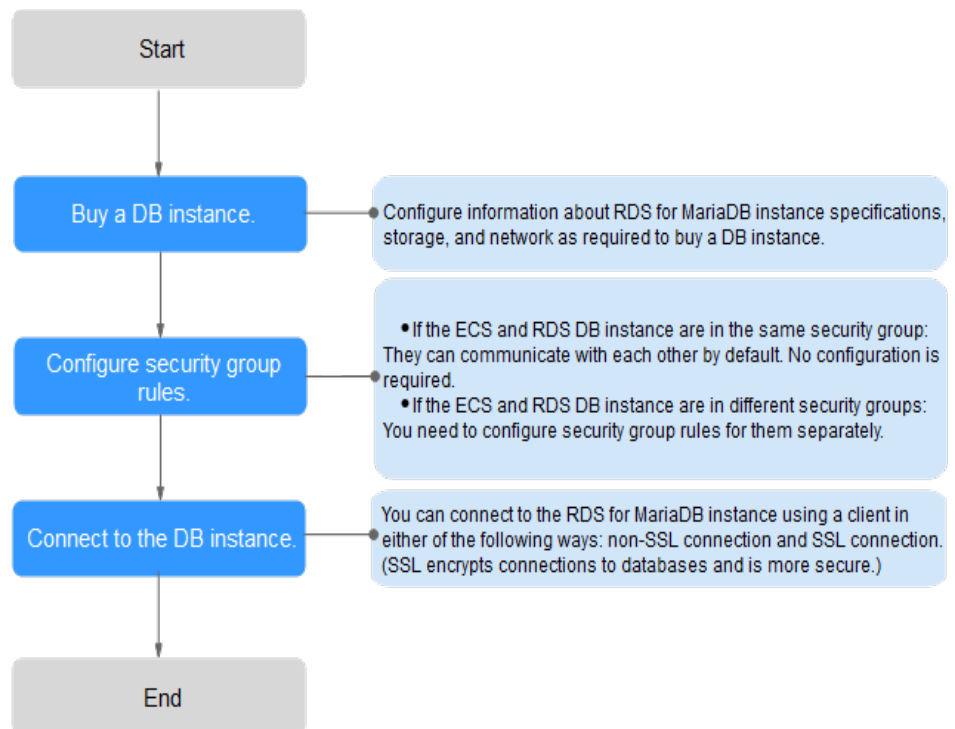
2.3.2 Connecting to a DB Instance Through a Private Network

2.3.2.1 Overview

Process

Figure 2-5 illustrates the process of connecting to an RDS for MariaDB instance through a private network.

Figure 2-5 Connecting to a DB instance through a private network



2.3.2.2 Configuring Security Group Rules

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS DB instance. This section describes how to configure an inbound rule for a DB instance.

Context

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted in a VPC.

Scenarios

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance Using a MariaDB Client](#).
- If they are in different security groups, configure security group rules for them, separately.
 - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
 - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

Constraints

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.


- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

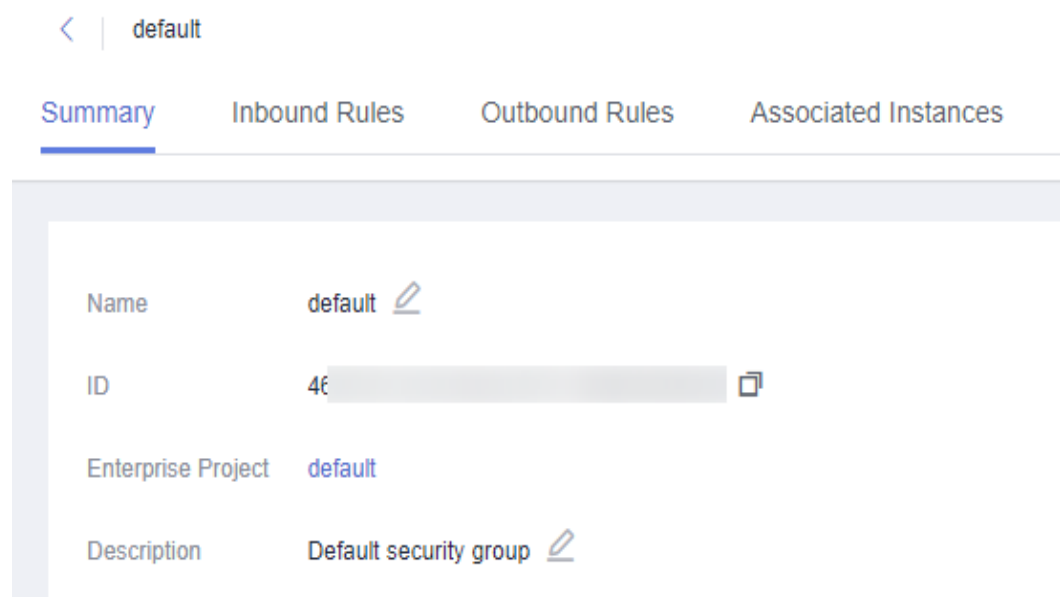
Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the DB instance name.

Step 4 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name.

Figure 2-6 Security group rules



Step 5 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.


To add more inbound rules, click  .

Table 2-9 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Security group rule action. Its value can be: <ul style="list-style-type: none"> • Allow: Access from the source is allowed to DB instances in the security group over specified ports. • Deny: Access from the source is denied to DB instances in the security group over specified ports. Deny rules take precedence over allow rules of the same priority.	Allow
Protocol & Port	Protocol : network protocol. Available options: All , TCP , UDP , ICMP , or GRE .	Protocols/TCP (Custom ports)
	Port : the port over which the traffic can reach your DB instance. RDS for MariaDB instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306
Type	Supported source IP address type. Its value can be: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4

Parameter	Description	Example Value
Source	<p>The source in an inbound rule is used to match the IP address or address range of an external request. The source can be:</p> <ul style="list-style-type: none"> • Single IP address: 192.168.10.10/32 (IPv4 address) • IP address segment: 192.168.1.0/24 (IPv4 address segment) • All IP addresses: 0.0.0.0/0 (any IPv4 address) • Security group: sg-abc • IP address group: ipGroup-test 	0.0.0.0/0
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).</p>	N/A

Step 6 Click **OK**.

----End

2.3.2.3 Connecting to a DB Instance Using a MariaDB Client

You can connect to a DB instance through a Secure Sockets Layer (SSL) connection or a non-SSL connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

Prerequisites

1. You have logged in to an ECS.
 - To connect to a DB instance through an ECS, you must ensure that:
 - The ECS and DB instance are in the same VPC.
 - The ECS is allowed by the security group to access the DB instance.
 - If the security group associated with the DB instance is the default security group, you do not need to configure security group rules.
 - If the security group associated with the DB instance is not the default security group, check whether the security group rules allow the ECS to connect to the DB instance. For details, see [Configuring Security Group Rules](#).

If the rules allow the access from the ECS, you can connect to the DB instance through the ECS.

If the rules do not allow the access from the ECS, you need to add a security group rule allowing the ECS to access the DB instance.


2. You have installed a database client to connect to DB instances.

You can use a database client to connect to the target DB instance in Linux or Windows.

- In Linux, install a **MariaDB client** on a device that can access RDS. It is recommended that you download a MariaDB client running a version later than that of the DB instance.


Connecting to a DB Instance Using Commands (SSL Connection)


Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the instance name to go to the **Basic Information** page.

Step 4 In the **DB Information** area, check whether SSL is enabled.

- If yes, go to **Step 5**.
- If no, click . In the displayed dialog box, click **OK**. Then, go to **6**.

Step 5 Click  next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.

Step 6 Import the root certificate **ca.pem** to the Linux or Windows.

Step 7 Connect to the RDS for MariaDB instance. In Linux, for example, run the following command:

- Method 1
`mysql -h <host> -P <port> -u <userName> -p --ssl-ca=<caName>`
 Example:
`mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=ca.pem`
- Method 2
`mysql -h <host> -P <port> -u <userName> -p --ssl-capath=<caPath>`

Table 2-10 Parameter description

Parameter	Description
<host>	Floating IP address. To obtain this parameter, go to the Basic Information page of the DB instance and view the floating IP address in the Connection Information area.

Parameter	Description
<port>	Database port. By default, the value is 3306 . To obtain this parameter, go to the Basic Information page of the DB instance and view the database port in the Connection Information area.
<userName>	Database account used for logging in to the DB instance. The default value is root .
<caName>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<caPath>	Path of the CA certificate.

Step 8 Enter the password of the database account if the following information is displayed:

Enter password:

Figure 2-7 Connection example

```
[root@xxxxxxxxxxxxxxxxxxxxx home]# mysql -h xxxxxxxxxxxxxxxxxxxx -P 3306 -u root -p --ssl-ca=/home/ca.pem
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19914
Server version: 10.5.16-221100-MariaDB-log MariaDB Community Server - (GPL)
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

----End

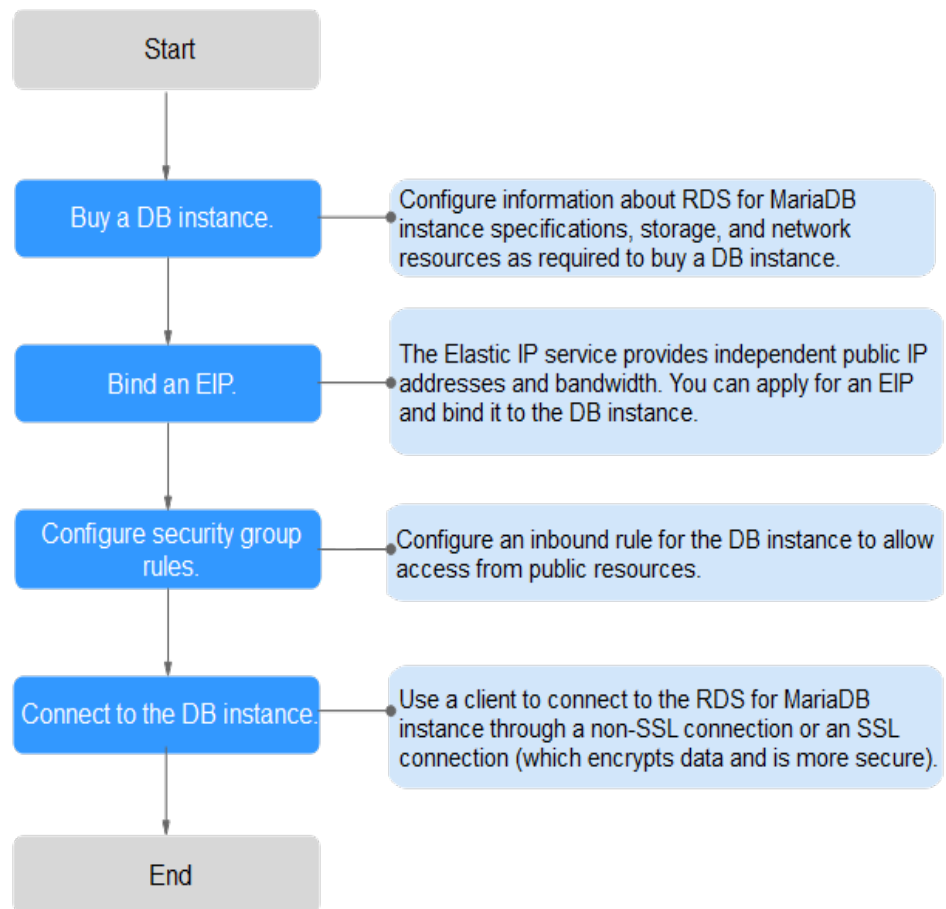
2.3.3 Connecting to a DB Instance Through a Public Network

2.3.3.1 Overview

Process

Figure 2-8 illustrates the process of connecting to an RDS for MariaDB instance through a public network.

Figure 2-8 Connecting to a DB instance through a public network



2.3.3.2 Binding an EIP

Scenarios


By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- To enable this function, contact customer service.
- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see [Configuring Security Group Rules](#).

Binding an EIP

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the target DB instance.

Step 4 In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.

Step 5 In the displayed dialog box, select an EIP and click **Yes**.

Step 6 On the **Connectivity & Security** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

2.3.3.3 Configuring Security Group Rules

For security, you need to create security group rules to allow specific IP addresses and ports to access your RDS DB instance. When you attempt to connect to an RDS DB instance through an EIP, configure an **inbound rule** for the security group associated with the DB instance.

Context

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted within a VPC.

Constraints

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.


- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

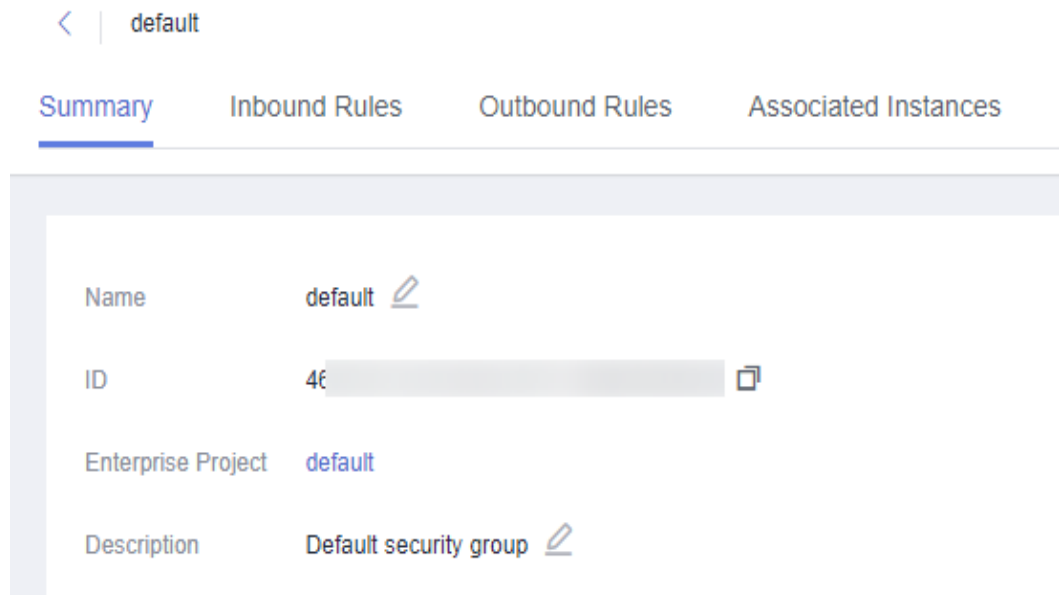
Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, click the DB instance name.

Step 4 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name.

Figure 2-9 Security group rules



Step 5 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.


To add more inbound rules, click .

Table 2-11 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1

Parameter	Description	Example Value
Action	<p>Security group rule action. Its value can be:</p> <ul style="list-style-type: none"> ● Allow: Access from the source is allowed to DB instances in the security group over specified ports. ● Deny: Access from the source is denied to DB instances in the security group over specified ports. <p>Deny rules take precedence over allow rules of the same priority.</p>	Allow
Protocol & Port	<p>Protocol: network protocol. Available options: All, TCP, UDP, ICMP, or GRE.</p>	Protocols/TCP (Custom ports)
	<p>Port: the port over which the traffic can reach your DB instance.</p> <p>RDS for MariaDB instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.</p>	3306
Type	<p>Supported source IP address type. Its value can be:</p> <ul style="list-style-type: none"> ● IPv4 ● IPv6 	IPv4
Source	<p>The source in an inbound rule is used to match the IP address or address range of an external request. The source can be:</p> <ul style="list-style-type: none"> ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test 	0.0.0.0/0

Parameter	Description	Example Value
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).</p>	N/A

Step 6 Click **OK**.

----End

2.3.3.4 Connecting to a DB Instance Using a MariaDB Client

You can connect to an instance through a non-SSL connection or an SSL connection using a MariaDB client. SSL encrypts connections to your DB instance and is more secure.

Prerequisites

1. An EIP has been bound to the target DB instance and security group rules have been configured. The operations are as follows:
 - a. Bind an EIP to your DB instance.
For details about how to bind an EIP, see [Binding an EIP](#).
 - b. Obtain the IP address of the ECS you use to connect to the DB instance.
 - c. Configure security group rules.
Add the IP address obtained in [1.b](#) and the DB instance port to the inbound rule of the security group.
For details about how to configure a security group rule, see [Configuring Security Group Rules](#).
 - d. Run the **ping** command to check the connectivity between the ECS and the EIP that has been bound to the DB instance in [1.a](#).
2. You have installed a database client to connect to DB instances.
You can use a database client to connect to the target DB instance in Linux or Windows.
 - In Linux, you need to install a [MariaDB client](#) on your device. It is recommended that you download a MariaDB client running a version later than that of the DB instance.
 - In Windows, you can use any common database client to connect to the target DB instance in a similar way.

Connecting to a DB Instance Using Commands (SSL Connection)

Step 1 Log in to the management console.




- Step 2** Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.
- Step 3** On the **Instances** page, click the instance name to go to the **Basic Information** page.
- Step 4** In the **DB Information** area, check whether SSL is enabled.
- If yes, go to **6**.
 - If no, click . In the displayed dialog box, click **OK**. Then, go to **6**.
- Step 5** Click  next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.
- Step 6** Import the root certificate **ca.pem** to the Linux or Windows.
- Step 7** Connect to the RDS for MariaDB instance. In Linux, for example, run the following command:
- Method 1
`mysql -h <host> -P <port> -u <userName> -p --ssl-ca=<caName>`
 Example:
`mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=ca.pem`
 - Method 2
`mysql -h <host> -P <port> -u <userName> -p --ssl-capath=<caPath>`

Table 2-12 Parameter description

Parameter	Description
<host>	EIP of the DB instance to be connected.
<port>	Port of the DB instance to be connected.
<userName>	Database account used for logging in to the DB instance. The default value is root .
<caName>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<caPath>	Path of the CA certificate.

- Step 8** Enter the password of the database account if the following information is displayed:

Enter password:

Figure 2-10 Connection example

```
[root@xxxxxxxxxxxxxxxxxx home]# mysql -h xxxxxxxxxxxxxxxxxxxx -P 3306 -u root -p --ssl-ca=/home/ca.pem
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19914
Server version: 10.5.16-221100-MariaDB-log MariaDB Community Server - (GPL)
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

 **NOTE**

If the connection fails, ensure that preparations have been correctly made in [Prerequisites](#) and try again.

----End


2.3.4 Connecting to a DB Instance Through DAS

Scenarios

Data Admin Service (DAS) enables you to connect to and manage DB instances with ease on a web-based console. The permission required for connecting to DB instances through DAS has been enabled for you by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.

Step 4 Enter the database username and password and click **Test Connection**.

Step 5 After the connection test is successful, click **Log In**.

----End

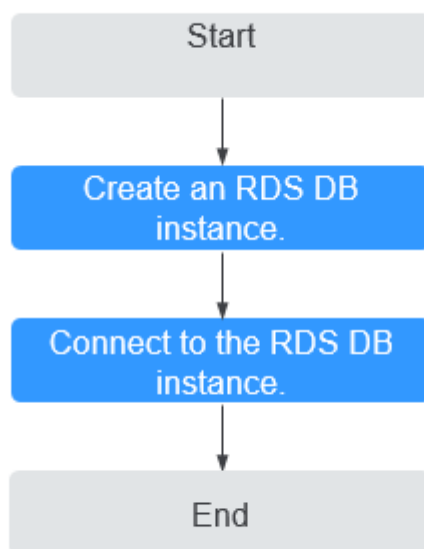
3 Getting Started with RDS for PostgreSQL

3.1 Operation Guide

You can create and connect to DB instances on the RDS console.

Flowchart

Figure 3-1 Flowchart



Procedure

Table 3-1 Related operations and references

Operation	Reference
Creating an RDS DB instance	Step 1: Buy a DB Instance
Connecting to an RDS DB instance	Step 2: Connect to a DB Instance

3.2 Step 1: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the RDS console.

RDS for PostgreSQL supports the yearly/monthly and pay-per-use billing modes. RDS allows you to tailor your compute resources and storage space to your business needs.

Procedure

- Step 1** Go to the [Buy DB Instance](#) page.
- Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.
- RDS provides the following billing modes:
 - **Yearly/Monthly**: If you select this mode, skip [Step 3](#) and go to [Step 4](#).
 - **Pay-per-use**: If you select this mode, go to [Step 3](#).
 - Basic information

Table 3-2 Basic information

Parameter	Description
Region	Region where your resources are located. NOTE Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.
DB Engine	Set to PostgreSQL .

Parameter	Description
DB Engine Version	Different DB engine versions are supported in different regions. You are advised to select the latest available version because it is more stable, reliable, and secure.
DB Instance Type	<ul style="list-style-type: none"> - Primary/Standby: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large and medium enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. - Single: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small- and medium-sized enterprises, or for learning about RDS.
Storage Type	Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be. <ul style="list-style-type: none"> - Ultra-high I/O: supports a maximum throughput of 350 MB/s. - Cloud SSD: cloud drives used to decouple storage from compute.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance.

- DB instance specifications

Table 3-3 Instance specifications

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes support different numbers of database connections and maximum IOPS.

Parameter	Description
Storage Space (GB)	Contains the file system overhead required for inode, reserved block, and database operation. Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB.
Disk Encryption	<ul style="list-style-type: none"> - Disable: indicates the encryption function is disabled. - Enable: indicates the encryption function is enabled, improving data security but affecting system performance. If you select Enable, Key Name indicating the tenant key needs to be specified. <p>NOTE</p> <ul style="list-style-type: none"> ▪ After an instance is created, the disk encryption status and the key cannot be changed. ▪ For details about how to create a key, see the "Creating a CMK" section in the <i>Key Management Service User Guide</i>.

- Network and database configuration

Table 3-4 Network

Parameter	Description
VPC	<p>A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details on how to create a VPC, see the "Creating a VPC" section in the <i>Virtual Private Cloud User Guide</i>.</p> <p>If no VPC is available, RDS allocates a VPC to you by default.</p> <p>NOTICE After a DB instance is created, the VPC cannot be changed.</p>
Subnet	<p>Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled.</p> <p>A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address.</p>

Parameter	Description
Security Group	<p>Controls the access that traffic has in and out of a DB instance. By default, the security group associated with the DB instance is authorized.</p> <p>Enhances security by controlling access to RDS from other services. You need to add inbound rules to a security group so that you can connect to your DB instance.</p> <p>If no security group is available, RDS allocates a security group to you by default.</p>

Table 3-5 Database configuration

Parameter	Description
Password	<ul style="list-style-type: none"> - Configure (default setting): Configure a password for your DB instance during the creation process. - Skip: Configure a password later after the DB instance is created. <p>NOTICE If you select Skip for Password, you need to reset the password before you can log in to the instance.</p>
Administrator	The default login name for the database is root .
Administrator Password	<p>Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#%&^*-_+?). Enter a strong password and periodically change it for security reasons.</p> <p>If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password.</p> <p>Keep this password secure. The system cannot retrieve it.</p>
Confirm Password	Must be the same as Administrator Password .

Parameter	Description
Parameter Template	<p>Contains engine configuration values that can be applied to one or more DB instances. If you intend to create primary/standby DB instances, they use the same parameter template.</p> <p>NOTICE If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used.</p> <ul style="list-style-type: none"> - maintenance_work_mem - shared_buffers - max_connections - effective_cache_size
Enterprise Project	If your account has been associated with an enterprise project, select the target project from the Enterprise Project drop-down list.

- Tags

Table 3-6 Tags

Parameter	Description
Tag	Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance.

- Purchase period

Table 3-7 Purchase period

Parameter	Description
Required Duration	This option is available only for yearly/monthly DB instances. The system will automatically calculate the configuration fee based on the selected required duration. The longer the required duration is, the larger discount you will enjoy.
Auto-renew	<ul style="list-style-type: none"> - This option is available only for yearly/monthly DB instances and is not selected by default. - If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	RDS supports batch creation of DB instances. If you intend to create primary/standby DB instances and set Quantity to 1 , a primary DB instance and a synchronous standby DB instance will be created.

 **NOTE**

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications for pay-per-use DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

Skip [Step 4](#) and [Step 5](#) and go to [Step 6](#).

Step 4 Confirm the order for yearly/monthly DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Pay Now**.

Step 5 Select a payment method and complete the payment.

 **NOTE**

This operation applies only to the yearly/monthly billing mode.

Step 6 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- The default database port is **5432**. You can change it after a DB instance is created.

----End

3.3 Step 2: Connect to a DB Instance

3.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 3-8 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address is required. You can connect to your DB instance through DAS on the management console.	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	<ul style="list-style-type: none"> • Easy to use, secure, advanced, and intelligent • Recommended
Private network	Floating IP	<p>RDS provides a floating IP address by default.</p> <p>When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.</p>	<ul style="list-style-type: none"> • Secure and excellent performance • Recommended

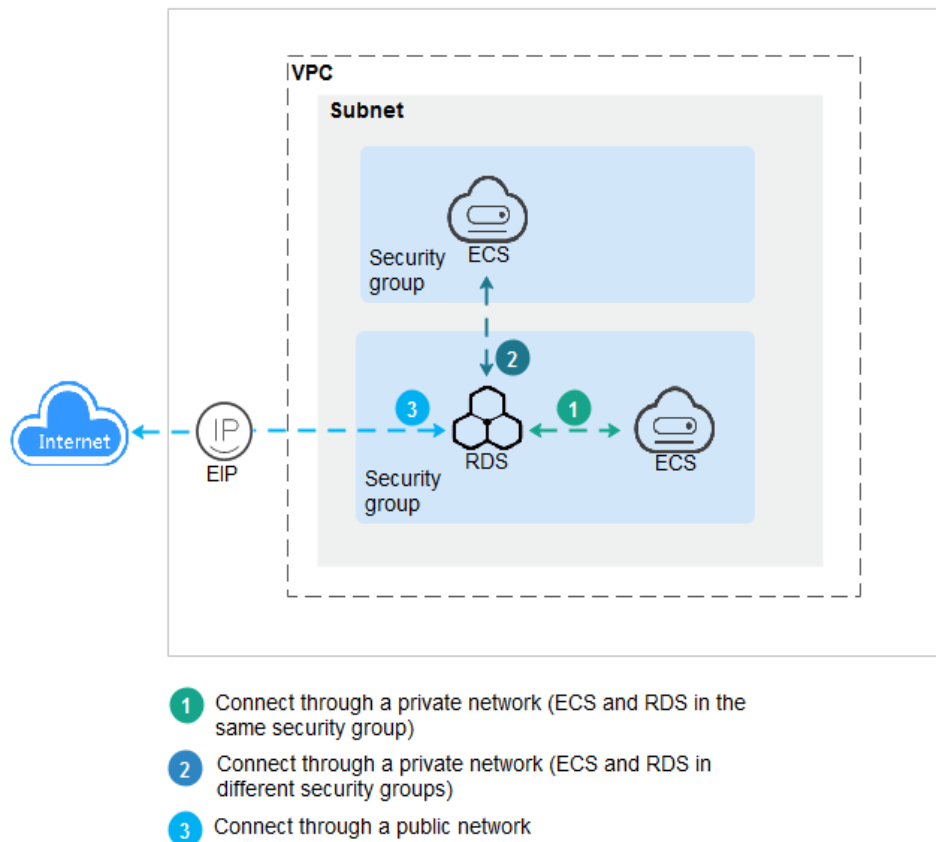
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	<ul style="list-style-type: none"> • A relatively lower level of security compared to other connection methods • To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance.

 **NOTE**

- VPC: indicates the Virtual Private Cloud.
- ECS: indicates the Elastic Cloud Server.
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 3-2 illustrates the connection over a private network or a public network.

Figure 3-2 DB instance connection




3.3.2 Connecting to a DB Instance Through DAS (Recommended)

Scenarios

Data Admin Service (DAS) enables you to connect to and manage databases with ease on a web-based console. The permissions required for connecting to DB instances through DAS are enabled by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page and choose **Databases > Relational Database Service**.

Step 3 On the **Instances** page, locate the DB instance and click **Log In** in the **Operation** column.

Alternatively, click the DB instance name on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner.

Step 4 On the displayed login page, enter the correct username and password and click **Log In**.

----End

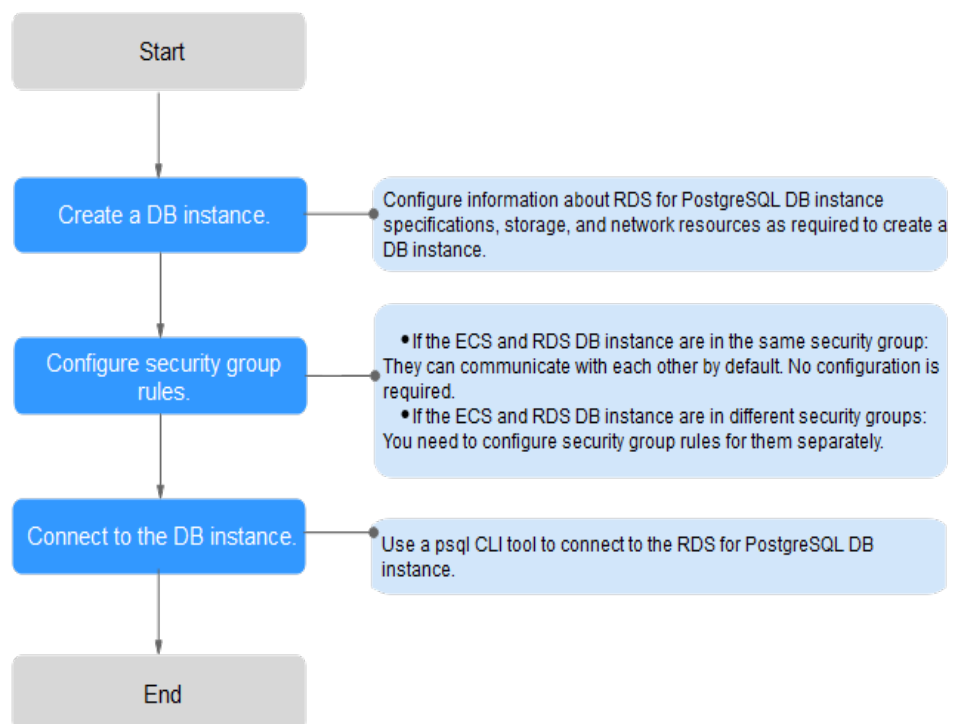
3.3.3 Connecting to a DB Instance Through a Private Network

3.3.3.1 Overview

Process

Figure 3-3 illustrates the process of connecting to an RDS for PostgreSQL DB instance through a private network.

Figure 3-3 Connecting to a DB instance through a private network



3.3.3.2 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a PostgreSQL client over a private network.

You can use the PostgreSQL client `psql` to connect to your DB instance over a Secure Sockets Layer (SSL) connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

Step 1: Buy an ECS

1. Log in to the management console and check whether there is an ECS available.
 - If there is a Linux ECS, go to [3](#).
 - If no Linux ECS is available, go to [2](#).
2. Buy an ECS and select Linux (for example, CentOS) as its OS.
To download a PostgreSQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for PostgreSQL DB instance for mutual communications.
For details about how to purchase a Linux ECS, see "Purchasing an ECS" in *Elastic Cloud Server User Guide*.
3. On the **ECS Information** page, view the region and VPC of the ECS.
4. On the **Basic Information** page of the RDS for PostgreSQL instance, view the region and VPC of the DB instance.
5. Check whether the ECS and RDS for PostgreSQL instance are in the same region and VPC.
 - If yes, go to [Step 2: Test Connectivity and Install a PostgreSQL Client](#).
 - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
 - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see "Changing a VPC" in the *Elastic Cloud Server User Guide*.

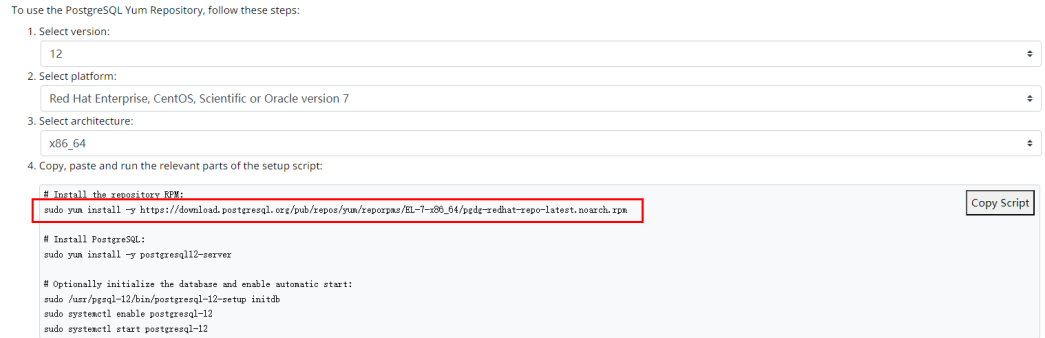
Step 2: Test Connectivity and Install a PostgreSQL Client

1. Log in to the ECS. For details, see "Login Using VNC" in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.
4. On the ECS, check whether the floating IP address and database port of the DB instance can be connected.
telnet 192.168.0.7 5432
 - If yes, network connectivity is normal.
 - If no, check the security group rules.
 - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.
 - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see [Configuring Security Group Rules](#).

5. Open the [client installation](#) page.
PostgreSQL provides [client installation methods](#) for different OSs on its official website.
The following describes how to install a PostgreSQL 12 client in CentOS.
6. Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client:

```
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

Figure 3-4 Installing a client



- Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
- Select an OS that is consistent with that of the ECS.
- Select an OS architecture that is consistent with that of the ECS.

Figure 3-5 Installing the RPM package

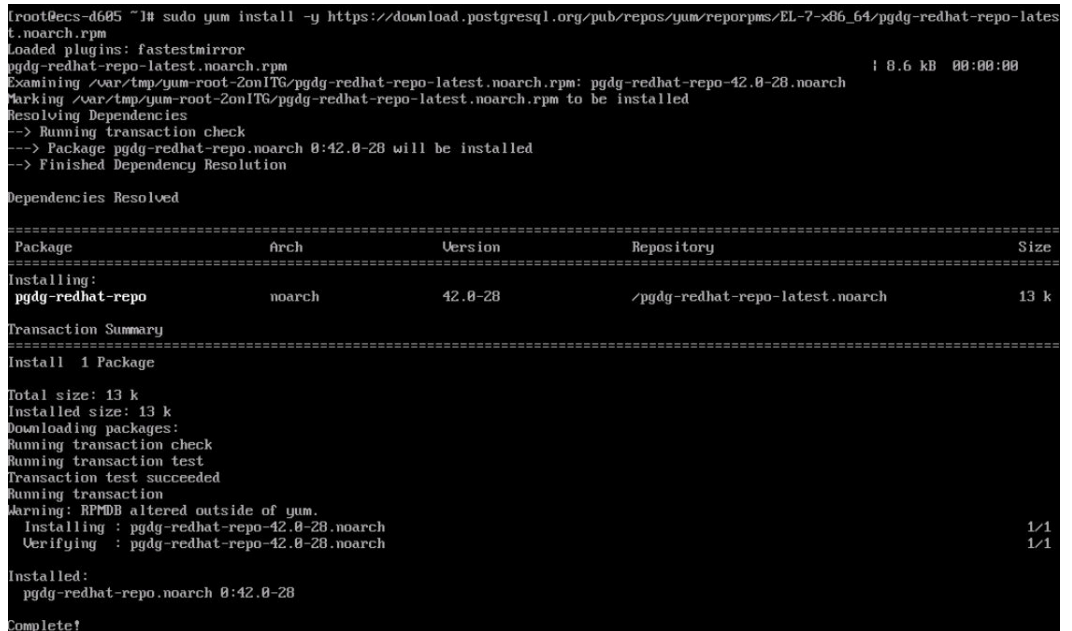


Figure 3-6 Client installed

```


Total
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Importing GPG key 0x442DF0F8:
  Userid : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
  Fingerprint: 68c9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
  Package : pgdg-redhat-repo-42.0-28.noarch (0/pgdg-redhat-repo-latest.noarch)
  From : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libicu-50.2.4.e17_7.x86_64 1/4
  Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 2/4
  Installing : postgresql12-12.13-1PGDG.rhel7.x86_64 3/4
  Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64 4/4
  Verifying : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 1/4
  Verifying : postgresql12-12.13-1PGDG.rhel7.x86_64 2/4
  Verifying : postgresql12-server-12.13-1PGDG.rhel7.x86_64 3/4
  Verifying : libicu-50.2.4.e17_7.x86_64 4/4

Installed:
  postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
  libicu.x86_64 0:50.2.4.e17_7 postgresql12.x86_64 0:12.13-1PGDG.rhel7 postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!
  
```

Step 3: Connect to the DB Instance Using Commands (SSL Connection)

1. On the **Instances** page, click the DB instance name.
2. In the navigation pane, choose **Connectivity & Security**.
3. In the **Connection Information** area, click  next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.
4. Upload **ca.pem** to the ECS.
5. Run the following command on the ECS to connect to the DB instance:

```
psql --no-readline -h <host> -p <port> "dbname=<database> user=<user> sslmode=verify-ca sslrootcert=<ca-file-directory>"
```

Example:

```
psql --no-readline -h 192.168.0.7 -p 5432 "dbname=postgres user=root sslmode=verify-ca sslrootcert=/root/ca.pem"
```

Table 3-9 Parameter description

Parameter	Description
<host>	Floating IP address obtained in 3 .
<port>	Database port obtained in 3 . The default value is 5432 .
<database>	Name of the database to be connected. The default database name is postgres .
<user>	Administrator account root .
<ca-file-directory>	Directory of the CA certificate used for the SSL connection. This certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to verify-ca to use a CA to check whether the service is trusted.

6. Enter the password of the database account as prompted.

Password:

If the following information is displayed, the connection is successful.

SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)

3.3.3.3 Configuring Security Group Rules

Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted within a VPC.

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to [Connecting to a DB Instance from a Linux ECS](#).
- If they are in different security groups, configure security group rules for them, separately.
 - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
 - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

- Step 1** Log in to the management console.
- Step 2** Under **Network**, click **Virtual Private Cloud**.
- Step 3** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 4** On the displayed page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 5** On the displayed page, click **Add Rule**.
- Step 6** In the displayed dialog box, set required parameters to add an inbound rule.
- Step 7** Click **OK**.

----End

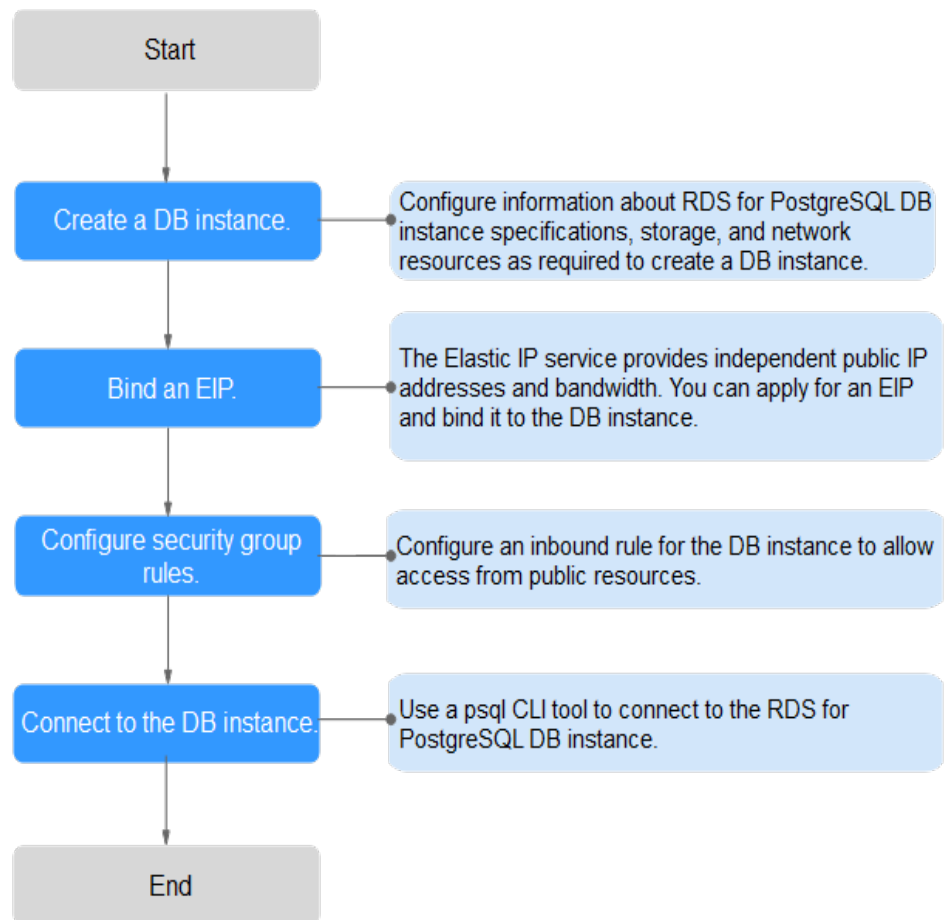
3.3.4 Connecting to a DB Instance Through a Public Network

3.3.4.1 Overview

Process

Figure 3-7 illustrates the process of connecting to an RDS for PostgreSQL DB instance through a public network.

Figure 3-7 Connecting to a DB instance through a public network



3.3.4.2 Binding an EIP

Scenarios

By default, a DB instance is not publicly accessible (not bound with an EIP) after being created. You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see section [Configuring Security Group Rules](#).
- Public accessibility reduces the security of DB instances. Therefore, exercise caution when deciding to connect to DB instances through a public network. To achieve a higher transmission rate and security level, you are advised to migrate your applications to the ECS that is in the same region as RDS.

Binding an EIP

- Step 1** Log in to the management console.
 - Step 2** On the **Instances** page, click the target DB instance.
 - Step 3** In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.
 - Step 4** In the displayed dialog box, select an EIP and click **Yes**.
If no available EIPs are displayed, click **View EIP** to obtain an EIP.
 - Step 5** On the **EIPs** page, view the EIP that has been bound to the DB instance.
You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.
- End

3.3.4.3 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a PostgreSQL client over a public network.

You can use the PostgreSQL client `psql` to connect to your DB instance over a Secure Sockets Layer (SSL) connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

Step 1: Buy an ECS

1. Log in to the management console and check whether there is an ECS available.
 - If there is a Linux ECS, go to [3](#).
 - If no Linux ECS is available, go to [2](#).
2. Buy an ECS and select Linux (for example, CentOS) as its OS.
To download a PostgreSQL client to the ECS, bind an EIP to the ECS.
For details about how to purchase a Linux ECS, see "Purchasing an ECS" in *Elastic Cloud Server User Guide*.
3. On the **ECS Information** page, view the region and VPC of the ECS.
4. On the **Basic Information** page of the RDS for PostgreSQL instance, view the region and VPC of the DB instance.

Step 2: Test Connectivity and Install a PostgreSQL Client

1. Log in to the ECS. For details, see "Login Using VNC" in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.
If no EIP has been bound to the DB instance, see [Binding an EIP](#).

- On the ECS, check whether the EIP and database port of the DB instance can be connected.

telnet *EIP 3306*

- If yes, network connectivity is normal.
- If no, check the security group rules.
 - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the EIP and port of the DB instance.
 - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see [Configuring Security Group Rules](#).

- Open the [client installation](#) page.

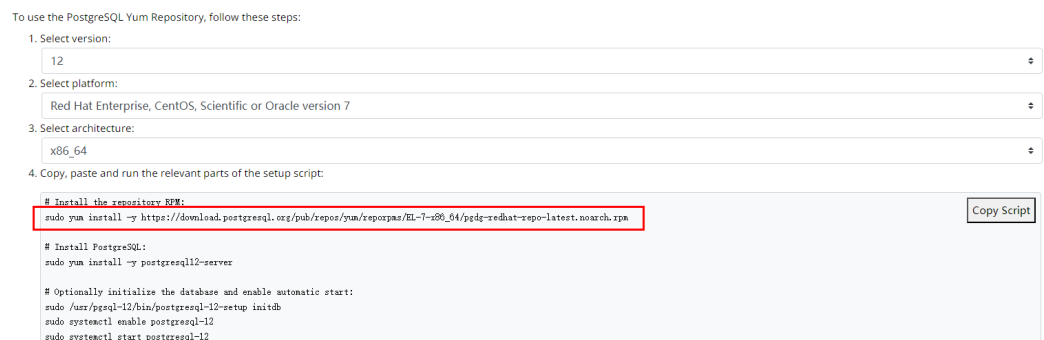
PostgreSQL provides [client installation methods](#) for different OSs on its official website.

The following describes how to install a PostgreSQL 12 client in CentOS.

- Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client:

```
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

Figure 3-8 Installing a client



- Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
- Select an OS that is consistent with that of the ECS.
- Select an OS architecture that is consistent with that of the ECS.

Figure 3-9 Installing the RPM package

```
[root@ecs-d685 ~]# sudo yum install -y https://download.postgresql.org/pub/repos/yum/repos/rpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
Loaded plugins: fastestmirror
Examining /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm: pgdg-redhat-repo-42.0-28.noarch
Marking /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
--> Package pgdg-redhat-repo.noarch 0:42.0-28 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                arch                Version             Repository           Size
=====
Installing:
pgdg-redhat-repo      noarch              42.0-28             /pgdg-redhat-repo-latest.noarch 13 k

Transaction Summary
=====
Install 1 Package

Total size: 13 k
Installed size: 13 k
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
Installing : pgdg-redhat-repo-42.0-28.noarch 1/1
Verifying  : pgdg-redhat-repo-42.0-28.noarch 1/1

Installed:
pgdg-redhat-repo.noarch 0:42.0-28

Complete!
```

Figure 3-10 Client installed


```
Total
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG 467 kB/s | 14 MB 00:00:30
Importing GPG key 0x442DF0F8:
  Userid : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
  Fingerprint: 60e9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
  Package : pgdg-redhat-repo-42.0-28.noarch (0/pgdg-redhat-repo-latest.noarch)
  From : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : libicu-58.2-4.el7_7.x86_64 1/4
Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 2/4
Installing : postgresql12-12.13-1PGDG.rhel7.x86_64 3/4
Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64 4/4
Verifying : postgresql12-libs-12.13-1PGDG.rhel7.x86_64 1/4
Verifying : postgresql12-12.13-1PGDG.rhel7.x86_64 2/4
Verifying : postgresql12-server-12.13-1PGDG.rhel7.x86_64 3/4
Verifying : libicu-58.2-4.el7_7.x86_64 4/4

Installed:
postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
libicu.x86_64 0:58.2-4.el7_7 postgresql12.x86_64 0:12.13-1PGDG.rhel7 postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!
```

Step 3: Connect to the DB Instance Using Commands (SSL Connection)

1. On the **Instances** page, click the DB instance name.
2. In the navigation pane, choose **Connectivity & Security**.
3. In the **Connection Information** area, click  next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.
4. Upload **ca.pem** to the ECS.
5. Run the following command on the ECS to connect to the DB instance:

```
psql --no-readline -h <host> -p <port> "dbname=<database> user=<user>
sslmode=verify-ca sslrootcert=<ca-file-directory>"
```

Example:

```
psql --no-readline -h 192.168.0.44 -p 5432 "dbname=postgres user=root
sslmode=verify-ca sslrootcert=/root/ca.pem"
```

Table 3-10 Parameter description

Parameter	Description
<i><host></i>	EIP obtained in 3 .
<i><port></i>	Database port obtained in 3 . The default value is 5432 .
<i><database></i>	Name of the database to be connected. The default database name is postgres .
<i><user></i>	Administrator account root .
<i><ca-file-directory></i>	Directory of the CA certificate used for the SSL connection. This certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to verify-ca to use a CA to check whether the service is trusted.

6. Enter the password of the database account as prompted.

Password:

If the following information is displayed, the connection is successful.

SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)

3.3.4.4 Configuring Security Group Rules

Scenarios

A security group is a collection of access control rules for ECSs and RDS DB instances that have the same security protection requirements and are mutually trusted within a VPC.

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

When you attempt to connect to an RDS DB instance through an EIP, you need to configure an **inbound rule** for the security group associated with the DB instance.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for each security group.

- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

 **NOTE**

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

- Step 1** Under **Network**, click **Virtual Private Cloud**.
- Step 2** In the navigation pane on the left, choose **Access Control > Security Groups**.
- Step 3** On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- Step 4** On the displayed page, click **Add Rule**.
- Step 5** In the displayed dialog box, set required parameters to add an inbound rule.
- Step 6** Click **OK**.

----End

A Change History

Released On	Description
2022-09-30	This issue is the first official release.